LG München I, Endurteil v. 25.11.2022 – 21 O 12142/21

Titel:

Begrenzung des patentrechtlichen Unverhältnismäßigkeitseinwands auf Ausnahmefälle

Normenketten:

EPÜ Art. 64 Abs. 1, Abs. 3

PatG § 139 Abs. 1 S. 1, S. 3, Abs. 2, § 140a Abs. 1, Abs. 3, § 140b Abs. 1, Abs. 3

Leitsätze:

1. Der Unverhältnismäßigkeitseinwand des § 139 Abs. 1 S. 3 PatG ist auf besondere Ausnahmefälle begrenzt, für deren Vorliegen der Patentverletzer darlegungs- und beweisbelastet ist (Fortführung von LG München I 5.8.2022 – 21 O 8879/21, GRUR-RS 2022, 34498 Rn. 82-84 - "keepawake-message"). (Rn. 87 – 89) (redaktioneller Leitsatz)

2. Der Umstand, dass der patentrechtliche Unterlassungsanspruch von einem Patentverwerter geltend gemacht wird, ist für sich genommen nicht geeignet, diesen als unverhältnismäßig einzustufen (Fortführung von LG München I 5.8.2022 – 21 O 8879/21, GRUR-RS 2022, 34498 Rn. 87 - "keepawake-message"). (Rn. 92) (redaktioneller Leitsatz)

3. Der Umstand, dass es sich bei den Verletzungsformen um komplexe Produkte handelt, führt nicht zu einer Unverhältnismäßigkeit der Geltendmachung des patentrechtlichen Unterlassungsanspruchs (Fortführung von LG München I 5.8.2022 – 21 O 8879/21, GRUR-RS 2022, 34498 Rn. 89-91 - "keepawake-message"). (Rn. 94 – 96) (redaktioneller Leitsatz)

Schlagwort:

Schadensersatz

Fundstellen:

MittdtPatA 2023, 552

LSK 2022, 42030

GRUR-RS 2022, 42030

Tenor

I. Die Beklagte wird verurteilt,

1. es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 - ersatzweise Ordnungshaft - oder einer Ordnungshaft bis zu sechs Monaten, im Falle wiederholter Zuwiderhandlungen bis zu insgesamt zwei Jahren, wobei die Ordnungshaft an den jeweiligen gesetzlichen Vertretern der Beklagten zu vollstrecken ist, zu unterlassen,

a) Funkkommunikationseinrichtungen

in der Bundesrepublik Deutschland anzubieten, in Verkehr zu bringen oder zu gebrauchen oder zu den genannten Zwecken einzuführen oder zu besitzen,

wobei die Funkkommunikationseinrichtungen umfassen:

Schlüsselentschlüsselungsmittel zum Entschlüsseln eines verschlüsselten ersten symmetrischen Schussels durch Verwenden eines geheimen Schlüssels, der in einer Sicherheitseinrichtung enthalten ist, die mit der Funkkommunikationseinrichtung verbunden ist, wobei der geheime Schlüssel ein zu einem öffentlichen Schlüssel gehörender privater Schlüssel ist und wobei der verschlüsselte erste symmetrische Schlüssel von einer anderen Funkkommunikationseinrichtung über eine Transfereinrichtung empfangen worden ist, und

ein Benutzerdatenentschlüsselungsmittel zum Entschlüsseln verschlüsselter Benutzerdaten mit dem entschlüsselten ersten symmetrischen Schlüssel, wobei die verschlüsselten Benutzerdaten von der anderen Funkkommunikationseinrichtung über die Transfereinrichtung empfangen worden sind, wobei die Benutzerdaten Benutzerdaten von der anderen Funkkommunikationseinrichtung sind, welche auf der Funkkommunikationseinrichtung wiederhergestellt werden sollen, wobei die Benutzerdaten persönliche,

private und hochsensible Daten des Benutzers der Funkkommunikationseinrichtung umfassen wie gespeicherte Nachrichten, Adressbucheinträge, Kalendereinträge und Kreditkartennummern;

(Anspruch 10 von … beschränkt)

b) Funkkommunikationseinrichtungen einer ersten Partei

in der Bundesrepublik Deutschland anzubieten, in Verkehr zu bringen oder zu gebrauchen oder zu den genannten Zwecken einzuführen oder zu besitzen,

wobei die Funkkommunikationseinrichtungen umfassen:

Schlüsselentschlüsselungsmittel zum Entschlüsseln eines verschlüsselten ersten symmetrischen Schüssels durch Verwenden eines geheimen Schlüssels, der in einer Sicherheitseinrichtung einer dritten Partei enthalten ist, die mit der Funkkommunikationseinrichtung verbunden ist, wobei der geheime Schlüssel nur der dritten Partei zur Verfügung steht und wobei der verschlüsselte erste symmetrische Schlüssel von einer anderen Funkkommunikationseinrichtung der ersten Partei über eine Transfereinrichtung empfangen worden ist, und

ein Benutzerdatenentschlüsselungsmittel zum Entschlüsseln verschlüsselter Benutzerdaten mit dem entschlüsselten ersten symmetrischen Schlüssel, wobei die verschlüsselten Benutzerdaten von der anderen Funkkommunikationseinrichtung über die Transfereinrichtung empfangen worden sind, wobei die Benutzerdaten Benutzerdaten von der anderen Funkkommunikationseinrichtung sind, welche auf der Funkkommunikationseinrichtung wiederhergestellt werden sollen, wobei die Benutzerdaten persönliche, private und hochsensible Daten des Benutzers der Funkkommunikationseinrichtung umfassen wie gespeicherte Nachrichten, Adressbucheinträge, Kalendereinträge und Kreditkartennummern;

(Anspruch 11 von … beschränkt)

c) Funkkommunikationseinrichtungen

in der Bundesrepublik Deutschland anzubieten, in Verkehr zu bringen oder zu gebrauchen oder zu den genannten Zwecken einzuführen oder zu besitzen,

wobei die Funkkommunikationseinrichtungen umfassen:

Schlüsselentschlüsselungsmittel zum Entschlüsseln eines verschlüsselten ersten symmetrischen Schussels durch Verwenden eines geheimen Schlüssels, der in einer Sicherheitseinrichtung enthalten ist, die mit der Funkkommunikationseinrichtung verbunden ist, wobei der geheime Schlüssel gegenüber der Funkkommunikationseinrichtung geheim gehalten wird und wobei der verschlüsselte erste symmetrische Schlüssel von einer anderen Funkkommunikationseinrichtung über eine Transfereinrichtung empfangen worden ist, und

ein Benutzerdatenentschlüsselungsmittel zum Entschlüsseln verschlüsselter Benutzerdaten mit dem entschlüsselten ersten symmetrischen Schlüssel, wobei die verschlüsselten Benutzerdaten von der anderen Funkkommunikationseinrichtung über die Transfereinrichtung empfangen worden sind, wobei die Benutzerdaten Benutzerdaten von der anderen Funkkommunikationseinrichtung sind, welche auf der Funkkommunikationseinrichtung wiederhergestellt werden sollen, wobei die Benutzerdaten persönliche, private und hochsensible Daten des Benutzers der Funkkommunikationseinrichtung umfassen wie gespeicherte Nachrichten, Adressbucheinträge, Kalendereinträge und Kreditkartennummern;

(Anspruch 12 von … beschränkt)

2. der Klägerin darüber Auskunft zu erteilen, in welchem Umfang sie (die Beklagte) die zu Ziffer 1.1. bezeichneten Handlungen seit dem 03.12.2015 begangen haben, und zwar unter Angabe

a) der Namen und Anschriften der Hersteller, Lieferanten und anderen Vorbesitzer,

b) der Namen und Anschriften der gewerblichen Abnehmer sowie der Verkaufsstellen, für die die Erzeugnisse bestimmt waren,

c) der Menge der ausgelieferten, erhaltenen oder bestellten Erzeugnisse sowie der Preise, die für die betreffenden Erzeugnisse bezahlt wurden,

wobei zum Nachweis der Angaben die entsprechenden Kaufbelege (nämlich Rechnungen, hilfsweise Lieferscheine) in Kopie vorzulegen sind,

wobei geheimhaltungsbedürftige Details außerhalb der auskunftspflichtigen Daten geschwärzt werden dürfen;

3. der Klägerin darüber Rechnung zu legen, in welchem Umfang sie die zu Ziffer 1.1. bezeichneten Handlungen seit dem 03.12.2015 begangen haben, und zwar unter Angabe

a) der einzelnen Lieferungen, aufgeschlüsselt nach Liefermengen, -zeiten und -preisen und der jeweiligen Typenbezeichnungen, sowie den Namen und Anschriften der gewerblichen Abnehmer;

b) der einzelnen Angebote, aufgeschlüsselt nach Angebotsmengen, -zeiten und -preisen und der jeweiligen Typenbezeichnungen sowie den Namen und Anschriften der gewerblichen Angebotsempfänger;

c) der betriebenen Werbung, aufgeschlüsselt nach Werbeträgern, deren Auflagenhöhe, Verbreitungszeitraum und Verbreitungsgebiet, im Fall von Internet-Werbung der Domain, der Zugriffszahlen und der Schaltungszeiträume jeder Kampagne;

d) der nach den einzelnen Kostenfaktoren aufgeschlüsselten Gestehungskosten und des erzielten Gewinns;

wobei der Beklagten vorbehalten bleibt, die Namen und Anschriften der nichtgewerblichen Abnehmer und Angebotsempfänger statt der Klägerin einem von der Klägerin zu bezeichnenden, ihr gegenüber zur Verschwiegenheit verpflichteten, in der Bundesrepublik Deutschland ansässigen, vereidigten Wirtschaftsprüfer mitzuteilen, sofern die Beklagte dessen Kosten tragen und ihn ermächtigen und verpflichten, der Klägerin auf konkrete Anfrage mitzuteilen, ob ein bestimmter Abnehmer oder Angebotsempfänger in der Aufstellung enthalten ist

und wobei die Rechnungslegungsdaten zusätzlich in einer mittels EDV auswertbaren elektronischen Form zu übermitteln sind;

4. die in ihrem unmittelbaren oder mittelbaren Besitz und/oder Eigentum befindlichen, vorstehend zu Ziffer 1.1. bezeichneten Erzeugnisse an einen von ihnen zu benennenden Gerichtsvollzieher zum Zweck der Vernichtung auf ihre - der Beklagten - Kosten herauszugeben;

5. die unter Ziffer 1.1. bezeichneten, seit 03.12.2015 in Verkehr gebrachten Erzeugnisse gegenüber den gewerblichen Abnehmern unter Hinweis auf den von der Kammer festgestellten patentverletzenden Zustand der Sache und mit der verbindlichen Zusage zurückzurufen, etwaige Entgelte zu erstatten sowie notwendige Verpackungs- und Transportkosten sowie mit der Rückgabe verbundene Zoll- und Lagerkosten zu übernehmen und die Erzeugnisse wieder an sich zu nehmen.

II. Es wird festgestellt, dass die Beklagte - gesamtschuldnerisch haftend mit … - verpflichtet ist, der Klägerin sämtliche Schäden zu ersetzen, die ihr durch die zu Ziffer 1.1. bezeichneten und seit dem 03.12.2015 begangenen Handlungen entstanden sind und noch entstehen werden.

III. Die Beklagte hat die Kosten des Rechtsstreits zu tragen.

IV. Das Urteil ist vorläufig vollstreckbar gegen Sicherheitsleistung in Höhe von

- 250.000,00 € einheitlich für Ziffer 1.1., I.4. und I.5.,

- 15.000,00 € einheitlich für Ziffern I.2. und I.3. sowie

- 110 % des jeweils zu vollstreckenden Betrags für Ziffer III.

Tatbestand

1
Die Klägerin ist Inhaberin des europäischen Patents … (Anlage K 1, nachfolgend: Klagepatent) und nimmt die Beklagte wegen unmittelbarer Patentverletzung in Anspruch.

2

Das Klagepatent wurde am 22.03.2004 angemeldet. Die Veröffentlichung und Bekanntmachung des Hinweises auf die Erteilung erfolgten am 21.04.2010. Das Klagepatent wurde mit Wirkung für Deutschland erteilt. Patentanspruch 10 des Klagepatents lautet in der erteilten Fassung im englischen Original wie folgt:

„A radio communication device (MS2), characterized in that the radio communication device (MS2) comprises:

key decryption means (K_DEC) for decrypting an encrypted first symmetric key by utiiizing a secret key comprised in a security device (SEC) connected to the radio communication device (MS2), the encrypted first symmetric key having been received from another radio communication device (MS1) via a transfer device (SERV), and

a user data decryption means (UD_DEC) for decrypting encrypted user data with the decrypted first symmetric key, the encrypted user data having been received from the another radio communication device (MS1) via the transfer device (SERV).“

3
Mit Entscheidung vom 08.07.2021 (Anlage K 2a) beschränkte das Deutsche Patent- und Markenamt (nachfolgend: DPMA) gemäß § 64 Abs. 1 PatG das Klagepatent entsprechend einem Beschränkungsantrag der Klägerin vom 01.06.2021 (Anlage K 2b). Aufgrund des Beschränkungsverfahrens wurde der nebengeordnete Anspruch 10 in den eingeschränkten nebengeordneten Anspruch 10 und die neuen eingeschränkten nebengeordneten Ansprüche 11 und 12 aufgespalten. Die eingeschränkten Ansprüche 10 bis 12 lauten wie folgt:

„10. A radio communication device (MS2), characterized in that the radio communication device (MS2) comprises:

- key decryption means (K_DEC) for decrypting an encrypted first symmetric key by utilizing a secret key comprised in a security device (SEC) connected to the radio communication device (MS2), the secret key being a private key associated with a public key, the encrypted first symmetric key having been received from another radio communication device (MS1) via a transfer device (SERV), and

- a user data decryption means (UD_DEC) for decrypting encrypted user data with the decrypted first symmetric key, the encrypted user data having been received from the another radio communication device (MS1) via the transfer device (SERV).

11. A radio communication device (MS2) of a first party, characterized in that the radio communication device (MS2) comprises:

- key decryption means (K_DEC) for decrypting an encrypted first symmetric key by utilizing a secret key comprised in a security device (SEC) of a third party connected to the radio communication device (MS2), the secret key only being available to the third party, the encrypted first symmetric key having been received from another radio communication device (MS1) via a transfer device SERV), and - a user data decryption means (UD_DEC] for decrypting encrypted user data with the decrypted first symmetric key, the encrypted user data having been received from the another radio communication device (MS1) via the transfer device (SERV).

12. A radio communication device (MS2), characterized in that the radio communication device (MS2) comprises:

- key decryption means (K_DEC) for decrypting an encrypted first symmetric key by utilizing a secret key comprised in a security device (SEC) connected to the radio communication device (MS2), the secret key being kept secret from the radio communication device, the encrypted first symmetric key having been received from another radio communication device (MS1) via a transfer device (SERV), and

- a user data decryption means (UD_DEC) for decrypting encrypted user data with the decrypted first symmetric key, the encrypted user, data having been received from the another radio communication device (MS1) via the transfer device (SERV).“

4
In dem durch Nichtigkeitsklage der Beklagten vom 01.12.2021 (Anlage HL 1) eingeleiteten Nichtigkeitsverfahren vor dem Bundespatentgericht stellte die Klägerin am 02.09.2022 einen Hilfsantrag

(Anlage K 26) mit einer weiteren Beschränkung der Ansprüche 10, 11 und 12 jeweils um folgende Merkmale:

„wherein the user data are user data from the another radio communication device (MS1) which are to be recovered on the radio communication device (MS2), and

wherein the user data comprise personal, private and highly sensitive data of the user of the radio communication device (MS2) such as saved messages, address book entries, calendar entries and credit card numbers."

5
Die nachfolgend eingeblendeten Abbildungen der Klagepatentschrift (Figuren 1 und 2) erläutern Ausführungsbeispiele der Erfindung:

6
Wegen der weiteren Details wird auf die Patentschrift verwiesen.

7
Die Beklagte stellt Smartphones her und vertreibt diese weltweit mit dem Betriebssystem Android. Dies betrifft insbesondere Smartphones mit den Modellbezeichnungen … (nachfolgend: angegriffene Ausführungsformen). Sie bietet sie auch in der Bundesrepublik Deutschland an, führt sie aus dem Ausland ins Inland ein und liefert sie im Inland an Kunden. Die anderweitig in Anspruch genommene … ist die europäische Niederlassung der Beklagten und tritt bei Käufen der angegriffenen Ausführungsformen im Inland über die Webseite der Beklagten als Verkäuferin auf.

8
Die Klägerin trägt vor, dass die von der Beklagten mit dem Betriebssystem Android vertriebenen Smartphones das Klagepatent in der vorliegend beschränkt geltend gemachten Fassung unmittelbar wortsinngemäß verletzten. Sie verweist hierzu auf Auszüge der Internetseiten https://developer.android.com/guide/topics/data/backup (Anlage K 7/K 7a) und https://developer.android.com/guide/topics/data/autobackup (Anlage K 8/K 8a) des Unternehmens Google als Hersteller des Android-Betriebssystems, die die Funktionen „Auto Backup" und „Key/Value Backup" betreffen, und die Beschreibung des zur Verschlüsselung und Entschlüsselung verwendeten System auf dem Google Security Blog unter https://security.googleblog.com/2018/10/google-and-android-have-your-back-by.html (Anlage K 10/K 10a). Daneben verweist die Klägerin auf den Bericht „Android Cloud Backup/Restore" vom 10.10.2018, abrufbar unter https://www.nccgroup.com/ae/our-research/android-cloudbackuprestore/ (Anlage K 11/K 11a, nachfolgend: NCC-Bericht). Der NCC-Bericht enthält unter anderem folgende grafische Darstellungen zum Backup-Prozess (dort S. 13/14, Figuren 7 und 8).

9
Die Klägerin ist der Ansicht, aufgrund der geltend gemachten Patentverletzung stünden ihr die entsprechenden Ansprüche, vor allem auch der Unterlassungsanspruch, zu.

10
Die Klägerin hat zunächst Ansprüche wegen Verletzung der Ansprüche 10, 11 und 12 in der durch das DPMA mit Entscheidung vom 08.07.2021 (Anlage K 2a) beschränkten Fassung geltend gemacht. Mit Schriftsatz vom 30.08.2022 hat die Klägerin Hilfsanträge zu den Unterlassungsanträgen aufgenommen entsprechend ihrem im Nichtigkeitsverfahren am 02.09.2022 gestellten Hilfsantrag (Anlage K 27). In der mündlichen Verhandlung am 07.09.2022 hat die Klägerin diese Hilfsanträge zum Hautantrag gemacht und den bisherigen Hauptantrag fallen gelassen (Bl. 301 d.A.).

11
Die Klägerin beantragt zuletzt,

I. die Beklagten zu verurteilen,

1. es bei Meidung eines für jeden Fall der Zuwiderhandlung vom Gericht festzusetzenden Ordnungsgeldes bis zu EUR 250.000,00 - ersatzweise Ordnungshaft - oder einer Ordnungshaft bis zu sechs Monaten, im Falle wiederholter Zuwiderhandlungen bis zu insgesamt zwei Jahren, wobei die Ordnungshaft an den jeweiligen gesetzlichen Vertretern der Beklagten zu vollstrecken ist, zu unterlassen,

a) Funkkommunikationseinrichtungen

in der Bundesrepublik Deutschland anzubieten, in Verkehr zu bringen oder zu gebrauchen oder zu den genannten Zwecken einzuführen oder zu besitzen,

wobei die Funkkommunikationseinrichtungen umfassen:

Schlüsselentschlüsselungsmittel zum Entschlüsseln eines verschlüsselten ersten symmetrischen Schussels durch Verwenden eines geheimen Schlüssels, der in einer Sicherheitseinrichtung enthalten ist, die mit der Funkkommunikationseinrichtung verbunden ist, wobei der geheime Schlüssel ein zu einem öffentlichen Schlüssel gehörender privater Schlüssel ist und wobei der verschlüsselte erste symmetrische Schlüssel von einer anderen Funkkommunikationseinrichtung über eine Transfereinrichtung empfangen worden ist, und

ein Benutzerdatenentschlüsselungsmittel zum Entschlüsseln verschlüsselter Benutzerdaten mit dem entschlüsselten ersten symmetrischen Schlüssel, wobei die verschlüsselten Benutzerdaten von der anderen Funkkommunikationseinrichtung über die Transfereinrichtung empfangen worden sind, wobei die Benutzerdaten Benutzerdaten von der anderen Funkkommunikationseinrichtung sind, welche auf der Funkkommunikationseinrichtung wiederhergestellt werden sollen, wobei die Benutzerdaten persönliche, private und hochsensible Daten des Benutzers der Funkkommunikationseinrichtung umfassen wie gespeicherte Nachrichten, Adressbucheinträge, Kalendereinträge und Kreditkartennummern,

(Anspruch 10 von … weiter beschränkt)

b) Funkkommunikationseinrichtungen einer ersten Partei

in der Bundesrepublik Deutschland anzubieten, in Verkehr zu bringen oder zu gebrauchen oder zu den genannten Zwecken einzuführen oder zu besitzen,

wobei die Funkkommunikationseinrichtungen umfassen:

Schlüsselentschlüsselungsmittel zum Entschlüsseln eines verschlüsselten ersten symmetrischen Schüssels durch Verwenden eines geheimen Schlüssels, der in einer Sicherheitseinrichtung einer dritten Partei enthalten ist, die mit der Funkkommunikationseinrichtung verbunden ist, wobei der geheime Schlüssel nur der dritten Partei zur Verfügung steht und wobei der verschlüsselte erste symmetrische Schlüssel von einer anderen Funkkommunikationseinrichtung über eine Transfereinrichtung empfangen worden ist, und ein Benutzerdatenentschlüsselungsmittel zum Entschlüsseln verschlüsselter Benutzerdaten mit dem entschlüsselten ersten symmetrischen Schlüssel, wobei die verschlüsselten Benutzerdaten von der anderen Funkkommunikationseinrichtung über die Transfereinrichtung empfangen worden sind, wobei die Benutzerdaten Benutzerdaten von der anderen Funkkommunikationseinrichtung sind, welche auf der Funkkommunikationseinrichtung wiederhergestellt werden sollen, wobei die Benutzerdaten persönliche, private und hochsensible Daten des Benutzers der Funkkommunikationseinrichtung umfassen wie gespeicherte Nachrichten, Adressbucheinträge, Kalendereinträge und Kreditkartennummern,

(Anspruch 11 von … weiter beschränkt)

c) Funkkommunikationseinrichtungen

in der Bundesrepublik Deutschland anzubieten, in Verkehr zu bringen oder zu gebrauchen oder zu den genannten Zwecken einzuführen oder zu besitzen,

wobei die Funkkommunikationseinrichtungen umfassen:

Schlüsselentschlüsselungsmittel zum Entschlüsseln eines verschlüsselten ersten symmetrischen Schussels durch Verwenden eines geheimen Schlüssels, der in einer Sicherheitseinrichtung enthalten ist, die mit der Funkkommunikationseinrichtung verbunden ist, wobei der geheime Schlüssel gegenüber der Funkkommunikationseinrichtung geheim gehalten wird und wobei der verschlüsselte erste symmetrische

Schlüssel von einer anderen Funkkommunikationseinrichtung über eine Transfereinrichtung empfangen worden ist, und

ein Benutzerdatenentschlüsselungsmittel zum Entschlüsseln verschlüsselter Benutzerdaten mit dem entschlüsselten ersten symmetrischen Schlüssel, wobei die verschlüsselten Benutzerdaten von der anderen Funkkommunikationseinrichtung über die Transfereinrichtung empfangen worden sind, wobei die Benutzerdaten Benutzerdaten von der anderen Funkkommunikationseinrichtung sind, welche auf der Funkkommunikationseinrichtung wiederhergestellt werden sollen, wobei die Benutzerdaten persönliche, private und hochsensible Daten des Benutzers der Funkkommunikationseinrichtung umfassen wie gespeicherte Nachrichten, Adressbucheinträge, Kalendereinträge und Kreditkartennummern,

(Anspruch 12 von … weiter beschränkt)

2. der Klägerin darüber Auskunft zu erteilen, in welchem Umfang sie (die Beklagten) die zu 1.1. bezeichneten Handlungen seit dem 03.12.2015 begangen haben, und zwar unter Angabe

a) der Namen und Anschriften der Hersteller, Lieferanten und anderen Vorbesitzer,

b) der Namen und Anschriften der gewerblichen Abnehmer sowie der Verkaufsstellen, für die die Erzeugnisse bestimmt waren,

c) der Menge der ausgelieferten, erhaltenen oder bestellten Erzeugnisse sowie der Preise, die für die betreffenden Erzeugnisse bezahlt wurden

wobei zum Nachweis der Angaben die entsprechenden Kaufbelege (nämlich Rechnungen, hilfsweise Lieferscheine) in Kopie vorzulegen sind,

wobei geheimhaltungsbedürftige Details außerhalb der auskunftspflichtigen Daten geschwärzt werden dürfen;

3. der Klägerin darüber Rechnung zu legen, in welchem Umfang sie die zu 1.1. bezeichneten Handlungen seit dem 03.12.2015 begangen haben, und zwar unter Angabe

a) der einzelnen Lieferungen, aufgeschlüsselt nach Liefermengen, -zeiten und -preisen und der jeweiligen Typenbezeichnungen, sowie den Namen und An-schriften der Abnehmer;

b) der einzelnen Angebote, aufgeschlüsselt nach Angebotsmengen, -zeiten und -preisen und der jeweiligen Typenbezeichnungen, sowie den Namen und Anschriften der gewerblichen Angebotsempfänger;

c) der betriebenen Werbung, aufgeschlüsselt nach Werbeträgern, deren Auflagenhöhe, Verbreitungszeitraum und Verbreitungsgebiet, im Falle von Internet-Werbung der Domain, der Zugriffszahlen und der Schaltungszeiträume jeder Kampagne;

d) der nach den einzelnen Kostenfaktoren aufgeschlüsselten Gestehungskosten und des erzielten Gewinns;

wobei

den Beklagten vorbehalten bleibt, die Namen und Anschriften der nichtgewerblichen Abnehmer und Angebotsempfänger statt der Klägerin einem von der Klägerin zu bezeichnenden, ihr gegenüber zur Verschwiegenheit verpflichteten, in der Bundesrepublik Deutschland ansässigen, vereidigten Wirtschaftsprüfer mitzuteilen, sofern die Beklagten dessen Kosten tragen und ihn ermächtigen und verpflichten, der Klägerin auf konkrete Anfrage mitzuteilen, ob ein bestimmter Abnehmer oder Angebotsempfänger in der Aufstellung enthalten ist;

und wobei die Rechnungslegungsdaten zusätzlich in einer mittels EDV auswertbaren elektronischen Form zu übermitteln sind;

4. die in ihrem unmittelbaren oder mittelbaren Besitz und/oder Eigentum befindlichen, vorstehend zu 1.1. bezeichneten Erzeugnisse an einen von ihnen zu benennenden Gerichtsvollzieher zum Zwecke der Vernichtung auf ihre - der Beklagten - Kosten herauszugeben;

5. die unter 1.1. bezeichneten, seit 03.12.2015 in Verkehr gebrachten Erzeugnisse gegenüber den gewerblichen Abnehmern unter Hinweis auf den von der Kammer festgestellten patentverletzenden Zustand der Sache und mit der verbindlichen Zusage zurückzurufen, etwaige Entgelte zu erstatten sowie notwendige

Verpackungs- und Transportkosten sowie mit der Rückgabe verbundene Zoll- und Lagerkosten zu übernehmen und die Erzeugnisse wieder an sich zu nehmen;

II. festzustellen, dass die Beklagten als Gesamtschuldner verpflichtet sind, der Klägerin sämtliche Schäden zu ersetzen, die ihr durch die zu 1.1. bezeichneten und seit dem 03.12.2015 begangenen Handlungen entstanden sind und noch entstehen werden.

12
Die Beklagte beantragt,

1. die Klage abzuweisen;

2. hilfsweise: den Rechtsstreit gemäß § 148 ZPO bis zu einer rechtskräftigen Entscheidung im Nichtigkeitsverfahren über den Rechtsbestand des deutschen Teils des Europäischen Patents EP … auszusetzen.

13
Die Klägerin wendet sich gegen eine Aussetzung des Verfahrens.

14
Die Beklagte ist im Wesentlichen der Ansicht, die angegriffenen Ausführungsformen verletzten das Klagepatent nicht. Jedenfalls sei das Verfahren im Hinblick auf die Nichtigkeitsklage vom 01.12.2021 (Anlage HL 1) auszusetzen. Die Aussprache eines Unterlassungsanspruchs sei hier unverhältnismäßig.

15
Zur Ergänzung des Tatbestands wird auf die eingereichten Schriftsätze samt Anlagen sowie auf die Sitzungsprotokolle vom 30.03.2022 (Bl. 141/144 d.A.) und 07.09.2022 (Bl. 299/301 d.A.) Bezug genommen.

Entscheidungsgründe

16
Die Klage ist zulässig (A.). Sie ist auch begründet. Die Beklagte benutzt den Gegenstand des Klagepatents (B.). Der Klägerin stehen gegen die Beklagte daher die nach Teilklagerücknahmen geltend gemachten Ansprüche vollumfänglich zu. Das Verfahren ist nicht nach § 148 ZPO auszusetzen (C.).

A.

17
Die Klage ist zulässig.

18
I. Das Landgericht München I ist zuständig (§ 143 PatG, § 32 ZPO i.V.m. § 38 Nr. 1 BayGZVJu, Art. 7 Nr. 2 EuGVVO).

19
II. Das erforderliche Feststellungsinteresse ist gegeben, § 256 Abs. 1 ZPO. Der Schadensersatzanspruch der Klägerin gegen die Beklagte ist vor Erteilung der Auskunft noch nicht bezifferbar.

B.

20
Die Klage ist begründet. Der Klägerin stehen gegen die Beklagte Ansprüche auf Unterlassung, Auskunft, Rechnungslegung, Vernichtung, Rückruf und Schadensersatzfeststellung gemäß §§ 139 Abs. 1 und 2, 140a Abs. 1 und 3, 140b Abs. 1 und 3, 9 S. 2 Nr. 1 PatG, §§ 242, 259 BGB i.V. mit Art. 64 Abs. 1 und 3 EPÜ zu.

21
I. Das Klagepatent betrifft den sicheren Transfer von Daten, insbesondere die Bereitstellung einer sicheren Datenübertragung von einer ersten Funkkommunikationseinrichtung auf eine zweite Funkkommunikationseinrichtung in Fällen, in denen die Datenübertragung von einer Transfereinrichtung einer anderen Partei überwacht werden soll, vgl. [0001].

22

1. In seiner Beschreibung führt die Klagepatentschrift aus, dass auf einer typischen Funkkommunikationseinrichtung zunehmend persönliche Benutzerdaten gespeichert seien, vgl. [0002].

23
Benutzerdaten seien typischerweise privat und könnten hochsensible Informationen enthalten, wie z.B. Kreditkartennummern, sodass das Bedürfnis bestehe, die Benutzerdaten vor einem unberechtigten Zugriff zu schützen. Die Klagepatentschrift beschreibt eine Situation, in der ein Benutzer sein beschädigtes oder ausgefallenes Funkkommunikationsgerät bei einer Servicestelle gegen ein neues Gerät austauscht. Hierbei würden typischerweise Benutzerdaten von der auszutauschenden Funkkommunikationseinrichtung auf die neue Funkkommunikationseinrichtung übertragen oder auf der neuen Funkkommunikationseinrichtung wiederhergestellt. Dieser Datentransfer werde typischerweise von dem Personal der Servicestelle überwacht, mithin einer anderen Person als dem Eigentümer des Geräts. Folglich müsse sichergestellt werden, dass auf die wiederherzustellenden Daten nicht durch das Personal der Servicestelle zugegriffen werden könne, sei es absichtlich oder unabsichtlich, vgl. [0003].

24
Im Stand der Technik würden die zu transferierenden Benutzerdaten typischerweise durch die von den Servicestelleneinrichtungen verwendete Software gescrambelt, sodass sie nicht mit standardmäßiger PC-Software geöffnet werden könnten, vgl. [0004].

25
2. Als nachteilig an dem aus dem Stand der Technik bekannten Schutz der Benutzerdaten kritisiert das Klagepatent, dass dieser schwach und leicht zu überwinden sei, vgl. [0004].

26
3. Vor diesem Hintergrund stellt sich das Klagepatent die Aufgabe, eine sichere Datenübertragung von einer ersten auf eine zweite Funkkommunikationseinrichtung bereitzustellen, vgl. [0005].

27
4. Hierfür schlägt das Klagepatent eine Funkkommunikationseinrichtung nach Maßgabe der zuletzt beschränkt geltend gemachten Ansprüche 10, 11 und 12 vor, die sich merkmalsmäßig wie folgt gliedern lassen:

Anspruch 10:

1. Funkkommunikationseinrichtung (MS2) umfassend:

2. Schlüsselentschlüsselungsmittel (K_DEC) zum Entschlüsseln

2.1 eines verschlüsselten ersten symmetrischen Schlüssels,

2.1.1 dieser ist von einer anderen Funkkommunikationseinrichtung (MS1) über eine Transfereinrichtung (SERV) empfangen worden;

2.2 durch Verwenden eines geheimen Schlüssels,

2.2.1 der in einer Sicherheitseinrichtung (SEC) enthalten ist,

2.2.2 die Sicherheitseinrichtung (SEC) ist mit der Funkkommunikationseinrichtung (MS2) verbunden und

2.2.3 der geheime Schlüssel ist ein zu einem öffentlichen Schlüssel gehörender privater Schlüssel;

3. Benutzerdatenentschlüsselungsmittel (DU_DEC) zum Entschlüsseln

3.1 verschlüsselter Benutzerdaten mit dem entschlüsselten ersten symmetrischen Schlüssel,

3.2 die verschlüsselten Benutzerdaten sind von der anderen Funkkommunikationseinrichtung (MS1) über die Transfereinrichtung (SERV) empfangen worden.

3.3 die Benutzerdaten sind Benutzerdaten von der anderen Funkkommunikationseinrichtung (MS1), welche auf der Funkkommunikationseinrichtung (MS2) wiederhergestellt werden sollen,

3.4 die Benutzerdaten umfassen persönliche, private und hochsensible Daten des Benutzers der Funkkommunikationseinrichtung (MS2) wie gespeicherte Nachrichten, Adressbucheinträge, Kalendereinträge und Kreditkartennummern.

Anspruch 11:

1. Funkkommunikationseinrichtung (MS2) einer ersten Partei umfassend:

2. Schlüsselentschlüsselungsmittel (K_DEC) zum Entschlüsseln

2.1 eines verschlüsselten ersten symmetrischen Schlüssels,

2.1.1 dieser ist von einer anderen Funkkommunikationseinrichtung (MS1) über eine Transfereinrichtung (SERV) empfangen worden;

2.2 durch Verwenden eines geheimen Schlüssels,

2.2.1 der in einer Sicherheitseinrichtung (SEC) einer dritten Partei enthalten ist,

2.2.2 die Sicherheitseinrichtung (SEC) ist mit der Funkkommunikationseinrichtung (MS2) verbunden und

2.2.3 der nur der dritten Partei zur Verfügung steht;

3. Benutzerdatenentschlüsselungsmittel (DU_DEC) zum Entschlüsseln

3.1 verschlüsselter Benutzerdaten mit dem entschlüsselten ersten symmetrischen Schlüssel,

3.2 die verschlüsselten Benutzerdaten sind von anderen Funkkommunikationseinrichtung (MS1) über die Transfereinrichtung (SERV) empfangen worden,

3.3 die Benutzerdaten sind Benutzerdaten von der anderen Funkkommunikationseinrichtung (MS1), welche auf der Funkkommunikationseinrichtung (MS2) wiederhergestellt werden sollen,

3.4 die Benutzerdaten umfassen persönliche, private und hochsensible Daten des Benutzers der Funkkommunikationseinrichtung (MS2) wie gespeicherte Nachrichten, Adressbucheinträge, Kalendereinträge und Kreditkartennummern.

Anspruch 12

1. Funkkommunikationseinrichtung (MS2) umfassend:

2. Schlüsselentschlüsselungsmittel (K_DEC) zum Entschlüsseln

2.1 eines verschlüsselten ersten symmetrischen Schlüssels,

2.1.1 dieser ist anderen Funkkommunikationseinrichtung (MS1) über eine Transfereinrichtung (SERV) empfangen worden;

2.2 durch Verwenden eines geheimen Schlüssels,

2.2.1 der in einer Sicherheitseinrichtung (SEC) enthalten ist,

2.2.2 die Sicherheitseinrichtung (SEC) ist mit der Funkkommunikationseinrichtung (MS2) verbunden und

2.2.3 der gegenüber der Funkkommunikationseinrichtung geheim gehalten wird;

3. Benutzerdatenentschlüsselungsmittel (DU_DEC) zum Entschlüsseln

3.1 verschlüsselter Benutzerdaten mit dem entschlüsselten ersten symmetrischen Schlüssel,

3.2 die verschlüsselten Benutzerdaten sind von anderen Funkkommunikationseinrichtung (MS1) über die Transfereinrichtung (SERV) empfangen worden

3.3 die Benutzerdaten sind Benutzerdaten von der anderen Funkkommunikationseinrichtung (MS1), welche auf der Funkkommunikationseinrichtung (MS2) wiederhergestellt werden sollen,

3.4 die Benutzerdaten umfassen persönliche, private und hochsensible Daten des Benutzers der Funkkommunikationseinrichtung (MS2) wie gespeicherte Nachrichten, Adressbucheinträge, Kalendereinträge und Kreditkartennummern.

5. Diese Lehre bedarf in Anspruch 10 hinsichtlich der Merkmale 2.1 i.V. mit 2.2 und 2.2.3, 2.2.1, 3.1, 3.2 und 3.3 sowie in Anspruch 11 hinsichtlich der Merkmale 2.2.1 und 2.2.3 näherer Erläuterung.

29
a) Die durch das Klagepatent unter Schutz gestellte technische Lehre ist aus Sicht der angesprochenen Durchschnittsfachperson, eines Diplomingenieurs der Nachrichtentechnik mit Universitätsabschluss mit mehrjähriger Erfahrung auf dem Gebiet der Datenverschlüsselung, zu ermitteln (Bl. 143 d.A.).

30
b) Die Funkkommunikationseinrichtung (MS2) gemäß Anspruch 10 umfasst nach Merkmal 2 Schlüsselentschlüsselungsmittel (K_DEC) zum Entschlüsseln eines verschlüsselten ersten symmetrischen Schlüssels gemäß Merkmal 2.1 durch Verwenden eines geheimen Schlüssels gemäß Merkmal 2.2, der gemäß Merkmal 2.2.3 ein zu einem öffentlichen Schlüssel gehörender privater Schlüssel ist.

31
aa) Merkmal 2.2 enthält - entgegen der Auffassung der Beklagten - keine Einschränkung dahingehend, dass der geheime Schlüssel zur unmittelbaren Entschlüsselung des ersten symmetrischen Schlüssels selbst verwendet wird. Vielmehr ist Merkmal 2.2 nach seinem Wortsinn bereits dann verwirklicht, wenn der geheime Schlüssel im Rahmen des Entschlüsselungsvorgangs des symmetrischen Schlüssels verwendet wird, was eine mittelbare Verwendung einschließt. Entgegen der Ansicht der Beklagten ist auch nicht erforderlich, dass der verschlüsselte erste symmetrische Schlüssel das Bezugsobjekt der - gegebenenfalls auch mehrlagigen - Entschlüsselung ist, d.h. sich die Verwendung des geheimen Schlüssels also gerade auf den verschlüsselten ersten symmetrischen Schlüssel bezieht. Dementsprechend muss der verschlüsselte erste symmetrische Schlüssel i.S. von Merkmal 2.1 - entgegen der Auffassung der Beklagten - auch nicht mit dem öffentlichen Schlüssel verschlüsselt worden sein, der zu dem geheimen Schlüssel gehört, zumal Anspruch 10 nur die Entschlüsselung betrifft, nicht auch die Verschlüsselung.

32
Eine derartige Einschränkung, wie die Beklagte meint, ist im Wortlaut und Wortsinn von Anspruch 10 nicht angelegt. Merkmal 2.2 setzt lediglich ein Entschlüsseln „durch Verwenden eines geheimen Schlüssels“ („by utilizing a secret key“) voraus. Eine unmittelbare Verwendung wird nicht verlangt. Demgegenüber verlangt Merkmal 3.1 explizit die Entschlüsselung verschlüsselter Benutzerdaten „mit dem entschlüsselten ersten symmetrischen Schlüssel“ („with the decrypted first symmetric key“).

33
Diesem systematischen Argument steht - entgegen der Ansicht der Beklagten - nicht entgegen, dass die Entschlüsselung in den Merkmalen 2.2 und 3.1 unterschiedlich gelöst ist. In Merkmalsgruppe 3 ist es das Benutzerdatenentschlüsselungsmittel (DU_DEC) selbst, das die Entschlüsselung der verschlüsselten Benutzerdaten durchführt, während in Merkmalsgruppe 2 das Schlüsselentschlüsselungsmittel (K_DEC) die Entschlüsselung des verschlüsselten ersten symmetrischen Schlüssels gerade nicht selbst durchführt, sondern sich hierzu einer separaten Funktionseinheit bedient, nämlich der Sicherheitseinrichtung (SEC), in und durch welche der verschlüsselte erste symmetrische Schlüssel entschlüsselt wird. So zeigt diese Unterscheidung der angesprochenen Fachperson an, dass die Formulierung des Entschlüsselns „durch Verwenden eines geheimen Schlüssels“ weiter zu verstehen ist und auch mittelbare Verwendungen umfasst.

34
Dieses Verständnis steht im Einklang mit der Erläuterung eines Ausführungsbeispiels unter Bezugnahme auf Figur 2 in [0034] bis [0036], wonach bei diesem Ausführungsbeispiel die Schlüsselentschlüsselungsmittel (K_DEC) unter anderem einen zweiten Schlüsselgenerator (KG2), ein Anfragenachrichtenmittel (REQ_MSG) und ein Antwortnachrichtenmittel (RESP_MSG) umfassen, so dass die Schritte zur Entschlüsselung des verschlüsselten ersten symmetrischen Schüssels, die das Schlüsselentschlüsselungsmittel im Ausführungsbeispiel vornimmt, unter anderem im Senden und Empfangen von Nachrichten liegen. Die eigentliche (unmittelbare) Entschlüsselung des ersten symmetrischen Schlüssels findet auf der Sicherheitseinrichtung (SEC) statt (vgl. [0035]), weil allein diese über den geheimen Schlüssel verfügt (vgl. Merkmal 2.2.1) und der geheime Schlüssel stets in der Sicherheitseinrichtung (SEC) verbleibt, d.h. insbesondere nicht an die Funkkommunikationseinrichtung (MS2) übermittelt wird. Die Entschlüsselung des ersten symmetrischen Schlüssels durch das Schlüsselentschlüsselungsmittel durch Verwenden des geheimen Schlüssels gemäß Merkmal 2.2 kann im Einklang mit diesem Ausführungsbeispiel nur mittelbar durch das Schlüsselentschlüsselungsmittel erfolgen, nämlich durch das Senden und Empfangen von Nachrichten, die für die Entschlüsselung von Relevanz

sind. Da auch dieses Ausführungsbeispiel vom Gegenstand der Erfindung erfasst sein muss, genügt es, wenn der geheime Schlüssel im Rahmen des Entschlüsselungsvorgangs des symmetrischen Schlüssels mittelbar verwendet wird.

35
Zudem enthält Anspruch 10 keine Beschränkung auf eine bestimmte Anzahl von Entschlüsselungsvorgängen, sondern ist insoweit offen und insbesondere nicht abschließend formuliert. So ist im Rahmen der Ausführungsbeispiele ebenfalls ausdrücklich die Nutzung eines zweiten symmetrischen Schlüssels vorgesehen (vgl. [0009], [0034]).

36
Auch funktional ist die von der Beklagten verfolgte Einschränkung des Wortsinns nicht geboten. Die aufgabengemäße Erhöhung der Sicherheit soll in Anspruch 10 dadurch bewirkt werden, dass zur Entschlüsselung des verschlüsselten ersten symmetrischen Schlüssels ein geheimer Schlüssel benötigt wird, der gemäß Merkmal 2.2.1 in einer Sicherheitseinrichtung (SEC) enthalten ist und somit besonders gegen unbefugten Zugriff gesichert ist (siehe hierzu sogleich). Für diese anspruchsgemäße Lösung kommt es nicht darauf an, ob der geheime Schlüssel unmittelbar zur Entschlüsselung des verschlüsselten ersten symmetrischen Schlüssels oder eines diesen Schlüssel enthaltenden Datenpakets als Bezugsobjekt der Entschlüsselung eingesetzt wird, sondern darauf, ob der verschlüsselte erste symmetrische Schlüssel nicht ohne Verwendung des geheimen Schlüssels entschlüsselt werden kann.

37
Etwas anderes folgt - entgegen der Ansicht der Beklagten - auch nicht aus der allgemeinen Patentbeschreibung in [0007] und [0008], weil [0007] jedenfalls - anders als Anspruch 10 - nicht den Vorgang der Entschlüsselung, sondern lediglich die (logisch vorgelagerte) Verschlüsselung betrifft, und [0008] für die Entschlüsselung die gleiche Formulierung wie Merkmal 2.2 („by utilizing a secret key“) enthält. Soweit die Beklagte daneben auf die Ausführungsbeispiele gemäß Figuren 1 und 2 verweist, schränken diese den Patentanspruch nicht ein.

38
Diese Auslegung entspricht auch der Rechtsprechung des Bundesgerichtshofs zu Zweckangaben in Patentansprüchen. Danach ist ein Patentanspruch, wenn er „die Eignung der geschützten Vorrichtung [fordert], einen bestimmten Vorgang ausführen zu können, und (…) ein Mittel [benennt], über das diese Eignung erreicht werden soll, (…) im Zweifel dahin auszulegen, dass das Mittel dazu vorgesehen ist und dementsprechend geeignet sein muss, an dem Vorgang, wenn er ausgeführt wird, in erheblicher Weise mitzuwirken“ (BGH GRUR 2020, 159, Rn. 18 - Lenkergetriebe). Dagegen ist es „nicht ausreichend, wenn ein Lenkergetriebe lediglich die Voraussetzungen dafür schafft“ (BGH a.a.O. Rn. 17 - Lenkergetriebe). Wie dargelegt (s.o.), versteht das Klagepatent den Vorgang des Entschlüsselns eines verschlüsselten ersten symmetrischen Schüssels in Merkmalsgruppe 2 weit und beschränkt diesen insbesondere nicht auf das eigentliche (unmittelbare) Entschlüsseln des ersten symmetrischen Schlüssels. Vielmehr umfasst der Vorgang auch Handlungen, die den eigentlichen Entschlüsselungsvorgang vorbereiten, etwa das Senden und Empfangen von Nachrichten, die die Entschlüsselung des ersten symmetrischen Schlüssels betreffen, vgl. [0034] bis [0036] (s.o.).

39
bb) Diese Auslegung der Merkmale 2.1 und 2.2 gilt gleichermaßen für die Ansprüche 11 und 12, die diese Merkmale wortgleich und keine Anhaltspunkte für eine Abweichung des Wortsinns enthalten.

40
cc) Nach Merkmal 2.2.3 ist der geheime Schlüssel ein zu einem öffentlichen Schlüssel gehörender privater Schlüssel, wobei der Begriff des geheimen Schlüssels einen Schlüssel beschreibt, der nur seinem Eigentümer zu Verfügung steht, und der Begriff des öffentlichen Schlüssels einen Schlüssel, der typischerweise öffentlich verfügbar ist, vgl. [0007].

41
c) Nach Merkmal 2.2.1 von Anspruch 10 (sowie ebenso von Anspruch 12) ist der gemäß Merkmal 2.1 verwendete Schlüssel in einer Sicherheitseinrichtung (SEC) enthalten.

42

Bei der Sicherheitseinrichtung kann es sich nach der Beschreibung beispielsweise um einen Server mit geeigneter Software handeln, vgl. [0031].

43
Entgegen der Ansicht der Beklagten muss die Sicherheitseinrichtung nach Merkmal 2.2.1 in Anspruch 10 nicht einer dritten Partei im Sinne einer Partei zugeordnet sein, der nicht zugleich die Transfereinrichtung (SERV) im Sinne von Merkmal 3.2 zugeordnet ist. Eine derartige Einschränkung ist in Anspruch 10 in Merkmal 2.2.1 nicht angelegt. Dieses enthält keine Aussage zur Zuordnung der Sicherheitseinrichtung. Hingegen sieht Anspruch 11 in Merkmal 2.2.1 gerade ausdrücklich eine „Sicherheitseinrichtung (SEC) einer dritten Partei“ vor.

44
Etwas anderes folgt - entgegen der Ansicht Beklagten - auch nicht aus dem technischen Hintergrund und der Aufgabe des Klagepatents. Dem Klagepatent geht es ausweislich der Beschreibung (unter anderem) um den Schutz der Benutzerdaten vor einem absichtlichen oder versehentlichen Zugriff auf die Benutzerdaten durch das Servicepersonal, das die Transfereinrichtung betreibt, vgl. [0003] und [0019]. Dieser Schutz wird anspruchsgemäß aber nicht dadurch umgesetzt, dass die Sicherheitseinrichtung und die Transfereinrichtung unterschiedlichen Parteien zugeordnet sein müssten, sondern dadurch, dass es sich bei der Sicherheitseinrichtung und der Transfereinrichtung um technisch getrennte Einheiten handelt.

45
Darüber hinaus würde die von der Beklagten geforderte Zuordnung der Sicherheitseinrichtung zu einer anderen Partei als der Partei, der die Transfereinrichtung zugeordnet ist, tatsächlich nicht zwangsläufig zu einem Mehr an Sicherheit bei Durchführung des Datentransfers zum einem Servicemitarbeiter führen, weil dem Servicemitarbeiter für die Durchführung des Datentransfers auch in der Auslegung der Beklagten Zugriff auf den geheimen Schlüssel in der Sicherheitseinrichtung gewährt werden müsste.

46
d) Die Funkkommunikationseinrichtung umfasst nach Merkmal 3 Benutzerdatenentschlüsselungsmittel (DU_DEC) zum Entschlüsseln verschlüsselter Benutzerdaten mit dem entschlüsselten ersten symmetrischen Schlüssel gemäß Merkmal 3.1. Merkmalsgruppe 3 ist für die eingeschränkten Ansprüche 10, 11 und 12 einheitlich gefasst und entsprechend einheitlich auszulegen.

47
Der Begriff der Benutzerdaten ist für sich genommen - entgegen der Ansicht der Klägerin - nicht dahingehend einschränkend auszulegen, dass Benutzerdaten zumindest die persönlichen, privaten und hochsensiblen Daten der Funkkommunikationseinrichtung umfassen. Anspruch 10 in der erteilten Fassung spricht diesbezüglich lediglich allgemein von „Benutzerdaten“ („user data“).

48
Auch die Beschreibung bietet keine Grundlage für eine einschränkende Auslegung. Zwar ist in der Erläuterung zum Hintergrund der Erfindung in [0002] und [0003] ausdrücklich von „persönlichen“ ([0002]: „personal“), „privaten“ ([0003]: „private“) und „hochsensiblen“ ([0003]: „highly sensitive“) Benutzerdaten bzw. Informationen die Rede, jedoch jeweils nur als typisches Beispiel (vgl. [0002]: „As a result a typical radio communication device contains more and more personal user data, such as saved messages, address book entries, calendar entries etc.“; [0003]: „Also typically user data is private and may contain highly sensitive information, such as credit card numbers etc.“, Hervorhebungen jeweils hinzugefügt).

49
Darüber hinaus spricht das Klagepatent in [0029] explizit die Möglichkeit an, dass die Benutzerdaten z.B. urheberrechtlich geschützte Inhalte oder vertrauliche Geschäftsunterlagen enthalten, bezüglich derer Zugangskontrollen von einer anderen als der ersten Partei etabliert wurden, befasst sich also mit einer Konstellation, in der es maßgeblich nicht auf die Privatheit der Benutzerdaten, sondern auf die Zuordnung der Daten zu einer anderen Person ankommt. Das Klagepatent offenbart (auch) hierfür eine Lösung. Dass das Klagepatent an dieser Stelle von „einigen der Benutzerdaten („some of the user data“) spricht, bedeutet daher - entgegen der Auffassung der Klägerin - nicht, dass der Begriff der Benutzerdaten für sich genommen zwangsläufig persönliche, private und hochsensible Daten des Benutzers umfasst.

50

Dass sich das Klagepatent ausdrücklich (auch) mit der Wiederherstellung der Benutzerdaten befasst (vgl. [0003]: „data recovery“; [0029]: „user data being restored“; [0033]: „recovering user data“), führt - entgegen dem Vortrag der Klägerin - ebenfalls zu keinem anderen Ergebnis. Eine Wiederherstellung kann sich gerade auch auf andere Daten als (persönliche) Benutzerdaten, die vom Benutzer stammen, beziehen, so z.B. auf die in [0029] ausdrücklich erwähnten zugangsbeschränkten und urheberrechtlich geschützten Inhalte.

51
e) Die von den Benutzerdatenentschlüsselungsmitteln gemäß Merkmal 3 zu entschlüsselnden Benutzerdaten sind nach Merkmal 3.2 von der anderen Funkkommunikationseinrichtung (MS1) über die Transfereinrichtung (SERV) empfangen worden.

52
Hierbei handelt es sich um dieselbe Transfereinrichtung wie die Transfereinrichtung, über die gemäß Merkmal 2.1.1 der verschlüsselte erste Schlüssel empfangen worden ist. Dies geht aus der Verwendung des bestimmten Artikels in Merkmal 3.2 („die Transfereinrichtung“ bzw. „the transfer device“) hervor, während die Transfereinrichtung in Merkmal 2.1.1 mit unbestimmtem Artikel in den Anspruch 10 eingeführt wird („eine Transfereinrichtung“ bzw. „a transfer device“). Jeweils wird auch die gleiche Abkürzung („SERV“) verwendet. Die Verwendung des bestimmten Artikels für die Transfereinrichtung gemäß Merkmal 3.2 findet sich zudem gleichermaßen in der Erläuterung zum Vorrichtungsanspruch 10 in [0017] im allgemeinen Teil der Beschreibung wieder. Im Ausführungsbeispiel gemäß Figur 1 wird die Transfereinrichtung für den verschlüsselten ersten Schlüssel und die verschlüsselten Benutzerdaten ebenfalls - wenn auch schematisch - als eine einzige Einheit („SERV“) dargestellt.

53
Die Transfereinrichtung kann nach einem Ausführungsbeispiel z.B. ein PC mit geeigneter Service-Software sein, vgl. [0031].

54
f) Nach dem - mit Hilfsantrag der Klägerin vom 02.09.2022 (Anlage K 26) im Nichtigkeitsverfahren ergänzten - Merkmal 3.3 sind die zu entschlüsselnden Benutzerdaten Benutzerdaten von der anderen Funkkommunikationseinrichtung (MS1), welche auf der Funkkommunikationseinrichtung (MS2) wiederhergestellt werden sollen.

55
Der Begriff der Wiederherstellung geht dabei über das bloße Übertragen der Benutzerdaten von der anderen Funkkommunikationseinrichtung (MS1) auf die Funkkommunikationseinrichtung (MS2) hinaus. Schon nach seinem Wortlaut beinhaltet der Begriff der Wiederherstellung mehr als die reine Übertragung. Vielmehr müssen die übertragenen Benutzerdaten auch verwendbar auf der Funkkommunikationseinrichtung (MS2) zur Verfügung stehen. Zudem wird in der Beschreibung die Wiederherstellung ausdrücklich als Alternative zur Übertragung benannt (vgl. [0003]: „transferred or recovered“, „data recovery or transfer“). Darüber hinaus geht aus der Erläuterung des Ausführungsbeispiels gemäß Figur 2 in [0031] hervor, dass die Wiederherstellung über das bloße Übertragen der Benutzerdaten hinausgeht, weil danach die Funkkommunikationseinrichtung (MS2) die „wiederherzustellenden Benutzerdaten“ empfängt („for receiving the user data to recovered“). Hierdurch wird verdeutlicht, dass der Wiederherstellungsvorgang in seiner Gesamtheit nicht mit dem Abschluss der Übertragung durch Empfang der Benutzerdaten bei der Funkkommunikationseinrichtung (MS2) endet, sondern zusätzlich jedenfalls einen nachgelagerten Aspekt der Wiederherstellung umfasst.

56
g) Anspruch 11 enthält in Merkmal 2.2.1 gegenüber Anspruch 10 - wie dort bereits erwähnt (s.o.) - die Einschränkung, dass die Sicherheitseinrichtung (SEC), in der der geheime Schlüssel enthalten ist, eine Sicherheitseinrichtung einer dritten Partei ist.

57
Hieraus folgt jedoch - entgegen der Ansicht der Beklagten - nicht, dass die Sicherheitseinrichtung (SEC) einer anderen Partei zugeordnet sein muss als die Transfereinrichtung (SERV). Zwar trifft es zu, dass in der Beschreibung der Klagepatentschrift, z.B. in [0001] und [0006], von der Transfereinrichtung einer zweiten Partei die Rede ist („transfer device of a second party“). Diese explizite Zuordnung hat jedoch - anders als beim Systemanspruch 6 - keinen Eingang in den erteilten Anspruch 10 und den beschränkt geltend

gemachten Anspruch 11 gefunden. Anspruch 11 enthält lediglich eine Zuordnung der Sicherheitseinrichtung (SEC) zu einer dritten Partei, die in Abgrenzung zu der ersten Partei zu verstehen ist, zu der gemäß Merkmal 1 von Anspruch 11 die Funkkommunikationseinrichtung (MS2) gehört. Dies impliziert nicht notwendigerweise die Existenz einer zweiten Partei.

58
Insbesondere bedeutet die Verwendung der Bezeichnung einer „dritten Partei“ in Merkmal 2.2.1 nicht, dass die Sicherheitseinrichtung einem anderen Unternehmen oder sogar einem anderen Konzern als die Transfereinrichtung zugeordnet sein muss. Vielmehr wird der angestrebte Schutz der Benutzerdaten - wie zur Auslegung von Merkmal 2.2.1 von Anspruch 10 dargelegt (s.o.) - anspruchsgemäß dadurch umgesetzt, dass es sich bei der Sicherheitseinrichtung und der Transfereinrichtung um technisch getrennte Einheiten handelt. Daneben spricht gegen die von der Beklagtenseite vorgenommene Auslegung, dass sie zu praktischen Problemen bei der technischen und/oder organisatorischen Umsetzung der anspruchsgemäßen Lösung in Konzernstrukturen führen würde. Schließlich würde die von der Beklagten geforderte Zuordnung der Sicherheitseinrichtung zu einer anderen Partei als der Partei, der die Transfereinrichtung zugeordnet ist, nicht zwangsläufig tatsächlich zu einem Mehr an Sicherheit bei Durchführung des Datentransfers durch einen Servicemitarbeiter führen, weil dem Servicemitarbeiter für die Durchführung des Datentransfers auch in der Auslegung der Beklagten Zugriff auf den geheimen Schlüssel in der Sicherheitseinrichtung gewährt werden müsste.

59
h) Nach Merkmal 2.2.3 von Anspruch 11 steht der geheime Schlüssel nur der dritten Partei zur Verfügung. Hinsichtlich des Begriffs der dritten Partei gilt das soeben zu Merkmal 2.2.1 Gesagte (s.o.). Dass der geheime Schlüssel „nur“ der dritten Partei zu Verfügung steht, verdeutlicht lediglich die bereits zu Merkmal 2.2.3 von Anspruch 10 dargelegte Auslegung des Begriffs des geheimen Schlüssels: Ein geheimer Schlüssel steht nur seinem Eigentümer zu Verfügung, vgl. [0007]. Insbesondere ist der geheime Schlüssel also nicht der Funkkommunikationseinrichtung der ersten Partei i.S. von Merkmal 1 des Anspruchs 11 bekannt.

60
II. Die Beklagte verletzt das Klagepatent unmittelbar gemäß § 9 S. 2 Nr. 1 PatG, weil sie die angegriffenen Ausführungsformen in der Bundesrepublik Deutschland anbietet und vertreibt und die angegriffenen Ausführungsformen durch Verwendung des Betriebssystems Android von den nunmehr weiter beschränkten Ansprüchen 10, 11 und 12 des Klagepatents unmittelbar wortsinngemäß Gebrauch machen.

61
1. Die Parteien streiten bezüglich Anspruch 10 über die Benutzung der Merkmale 2.1 i.V. mit 2.2 und 2.2.3, 2.2.1 und 3.2 sowie die entsprechenden Merkmale in den Ansprüchen 11 und 12, soweit sie wortgleich formuliert sind. Bezüglich Anspruch 11 streiten die Parteien außerdem über die Benutzung der - gegenüber Anspruch 10 abweichend formulierten - Merkmale 2.2.1 und 2.2.3. Gegen die Benutzung der übrigen Merkmale wendet sich die Beklagte zu Recht nicht. Denn diese werden nach dem unstreitigen Vortrag der Klägerin von den angegriffenen Ausführungsformen verwirklicht.

62
2. Die angegriffenen Ausführungsformen verwirklichen Merkmal 2.1 i.V. mit 2.2 und 2.2.3 von Anspruch 10.

63
Im Rahmen des im NCC-Bericht (Anlage K 11/K 11a) geschilderten Backup-Prozesses des Android-Betriebssystems wird der als verschlüsselter erster symmetrischer Schlüssel anzusehende Tertiary Key (Merkmals 2.1) durch Verwenden des geheimen Schlüssels Cohort Private Key (cohort_sk) entschlüsselt (Merkmal 2.2), der ein zu dem öffentlichen Schlüssel Cohort Public Key (cohort_pk) gehörender privater Schlüssel ist (Merkmal 2.2.3).

64
Zwischen den Parteien ist für sich genommen unstreitig, dass es sich bei dem Tertiary Key um einen verschlüsselten symmetrischen Schlüssel handelt (Merkmal 2.1) und der Cohort Private Key ein zu dem öffentlichen Schlüssel Cohort Public Key gehörender privater Schlüssel ist (Merkmal 2.2.3).

65

Nach Ansicht der Beklagten werde der Cohort Private Key aber nicht zum Entschlüsseln des Tertiary Key i.S. von Merkmal 2.2 verwendet. Die Beklagtenseite verweist dabei zur Erläuterung auf eine von ihr folgendermaßen ergänzte Version der Figur 8 auf Seite 14 des NCC-Berichts (vgl. Klageerwiderung, S. 22):

66
Mit dem Cohort Private Key werde nicht der Tertiary Key entschlüsselt, sondern der THM_encrypted_recovery_key. Der Cohort Private Key werde damit nicht zur Entschlüsselung des verschlüsselten ersten symmetrischen Schlüssels verwendet, sondern für einen völlig anderen Entschlüsselungsvorgang im Zusammenhang mit dem Recovery Key. Der Tertiary Key werde nur einmal verschlüsselt und zwar mit dem (unverschlüsselten) Application Key/Secondary Key. Im Anschluss werde der verschlüsselte Tertiary Key auf einem Anwendungsserver gespeichert. Alle weiteren Verschlüsselungsebenen beträfen Application Key/Secondary Key bzw. den Recovery Key. Es liege damit gerade keine mehrlagige Verschlüsselung des Tertiary Key vor. Dementsprechend liege auch keine korrespondierende mehrlagige Entschlüsselung des verschlüsselten Tertiary Key vor. Der Cohort Private Key werde zur Entschlüsselung einer Verschlüsselungslage des THM_encrypted_recovery_key verwendet. In diesem Schlüssel sei nach Entfernung sämtlicher Entschlüsselungsschichten (einschließlich der Zwischenverschlüsselungsschicht durch den key_claimant) jedoch nicht der Tertiary Key enthalten. Nach Entfernung sämtlicher Verschlüsselungsschichten des THM_encrypted_recovery_key erhalte man vielmehr den Recovery Key. Der Recovery Key werde sodann verwendet, um den verschlüsselten Application Key (encrypted_application_key) zu entschlüsseln. Auch in dem verschlüsselten Application Key (encrypted_application_key) sei der erste symmetrische Schlüssel nicht enthalten.

67
Diese Argumentation der Beklagtenseite greift nicht durch. Wie im Rahmen der Auslegung dargelegt (s.o.), setzt die Verwirklichung der Merkmale 2.1 und 2.2 weder voraus, dass der Cohort Private Key als geheimer Schlüssel unmittelbar zur Entschlüsselung des Tertiary Key als verschlüsselten ersten symmetrischen Schlüssels eingesetzt wird, noch, dass ein diesen Schlüssel enthaltendes Datenpaket Bezugsobjekt der Entschlüsselung ist. Spiegelbildlich muss der verschlüsselte erste symmetrische Schlüssel i.S. von Merkmal 2.1 auch nicht mit dem öffentlichen Schlüssel verschlüsselt worden sein, der zu dem geheimen Schlüssel gehört. Vielmehr kommt es darauf an, dass im Rahmen des - weit zu verstehenden - Entschlüsselungsvorgangs der verschlüsselte erste symmetrische Schlüssel nicht ohne Verwendung des geheimen Schlüssels entschlüsselt werden kann. Dies ist bei dem im NCC-Bericht beschriebenen Backup-Prozess des Android-Betriebssystems unstreitig der Fall.

68
3. Die angegriffenen Ausführungsformen machen auch von Merkmal 2.2.1 des Anspruchs 10 Gebrauch.

69
Der Cohort Private Key als geheimer Schlüssel ist im Google Cloud Key Vault enthalten, das ausweislich des NCC-Berichts (Anlage K 11/K 11 a) über separate Server und eine besondere Sicherheitshard- und -software verfügt (dort, S. 7/9). Dies stellt eine Sicherheitseinrichtung i.S. von Merkmal 2.2.1 dar, wie aus Beschreibungsstelle [0031] hervorgeht, in der beispielhaft ein Server mit geeigneter Software („The security device SEC may be e.g. a server with suitable software.“) gezeigt ist.

70
Es handelt sich bei dem Google Cloud Key Vault auch - was insoweit unstreitig ist - um eine von der als Transfereinrichtung (SERV) einzustufenden Entität, die von der Klägerseite als „Google Drive“ und von der Beklagtenseite als „Anwendungsserver“ bezeichnet wird, technisch getrennte Entität.

71
Dass das Google Cloud Key Vault ebenso wie die Server, auf denen die verschlüsselten Benutzerdaten gespeichert werden, Google zugeordnet ist, steht - entgegen der Ansicht der Beklagten - einer Verwirklichung von Merkmal 2.2.1 nicht entgegen. Wie im Rahmen der Auslegung dargelegt (s.o.), muss die Sicherheitseinrichtung nach Merkmal 2.2.1 in Anspruch 10 gerade nicht einer anderen Partei zugeordnet sein als der Partei, der die Transfereinrichtung i.S. von Merkmal 3.2 zugeordnet ist, über die die Funkkommunikationseinrichtung (MS2) die verschlüsselten Benutzerdaten empfängt.

72
4. Merkmal 3.2 wird durch die angegriffenen Ausführungsformen ebenfalls verwirklicht.

73
Der als verschlüsselter erster symmetrischer Schlüssel i.S. von Merkmal 2.1 anzusehende Tertiary Key (s.o.) und die verschlüsselten Benutzerdaten werden - was insoweit unstreitig ist - über die gleiche technische Entität übertragen. Die Klägerseite bezeichnet diese technische Entität mit „Google Drive“, die Beklagtenseite spricht von einem „Anwendungsserver“, was in der Sache keinen Unterschied macht. Es handelt sich jedenfalls um die gleiche Transfereinrichtung (SERV) i.S. von Merkmal 2.1.1 und Merkmal 3.2. Die Beklagtenseite stützt ihr Nichtverletzungsargument hinsichtlich Merkmal 3.2 auf die Annahme, dass der Tertiary Key nicht den verschlüsselten ersten symmetrischen Schlüssel i.S. von Merkmal 2.1 darstelle. Da diese Ansicht - wie gezeigt (s.o.) - nicht zutrifft, verbleibt in Bezug auf Merkmal 3.2 kein gesondertes Nichtverletzungsargument der Beklagten.

74
5. Auch in Bezug auf Anspruch 11 machen die angegriffenen Ausführungsformen von Merkmal 2.2.1 Gebrauch.

75
Bei dem Google Cloud Key Vault handelt es sich um eine Sicherheitseinrichtung (SEC) einer dritten Partei i.S. von Merkmal 2.2.1 des Anspruchs 11. Die angegriffenen Ausführungsformen als Funkkommunikationseinrichtungen (MS2) i.S. von Merkmal 1 gehören jeweils ihrem Nutzer und damit einer ersten Partei. Das Google Cloud Key Vault als Sicherheitseinrichtung ist dem Google Cloud Key Vault Service und somit einer dritten Partei zuzuordnen.

76
Dass der Google Cloud Key Vault Service wie die Transfereinrichtung (Google Drive bzw. Anwendungsserver) zu Google gehört, steht einer Verwirklichung von Merkmal 2.2.1 des Anspruchs 11 nicht entgegen, da nach zutreffender Auslegung (s.o.) eine Zuordnung zu einer anderen Partei als der Partei, der die Transfereinrichtung zugeordnet ist, nicht erforderlich ist. Wie bezüglich Merkmal 2.2.1 des Anspruchs 10 (s.o.) ist vielmehr entscheidend, dass es sich bei Sicherheitseinrichtung und Transfereinrichtung um technisch getrennte Einheiten handelt, was vorliegend gegeben ist.

77
6. Schließlich steht der Cohort Private Key als geheimer Schlüssel nur dem Google Cloud Key Vault Service und folglich - wie soeben zu Merkmal 2.2.1 erläutert - nur der dritten Partei i.S. von Merkmal 2.2.3 des Anspruchs 11 zur Verfügung.

78
III. Die Beklagtenseite ist passivlegitimiert.

79
IV. Damit stehen der Klägerin die geltend gemachten Ansprüche im tenorierten Umfang zu.

80
1. Der Anspruch auf Unterlassung folgt aus Art. 64 Abs. 1 EPÜ, § 139 Abs. 1 PatG.

81
a) Die Wiederholungsgefahr wird durch die festgestellten rechtswidrigen Benutzungshandlungen indiziert.

82
b) Der Unterlassungsanspruch ist nicht aus Gründen der Unverhältnismäßigkeit ausgeschlossen, § 139 Abs. 1 S. 3 PatG. Er ist verhältnismäßig, § 139 Abs. 1 S. 3 PatG.

83
aa) Die Beklagtenseite meint, ein Totalverbot wäre unverhältnismäßig, da die Interessen der Klägerin vornehmlich in der Monetarisierung des Klagepatents, nicht in der Vermarktung ihrer technischen Errungenschaften lägen und gegenüber den Interessen der Beklagtenseite zurückstehen müssten. Ein Totalverbot hätte für die Beklagtenseite wirtschaftliche Auswirkungen, die völlig außer Verhältnis zum Anteil des Klagepatents an den technisch komplexen Produkten der angegriffenen Ausführungsformen stünden. Dies gelte insbesondere aufgrund des Umstands, dass die Produkte der Beklagtenseite komplexe Produkte

seien und das Klagepatent nur eine verschwindend geringe, überdies von Dritten bereitgestellte Teilfunktion des Gesamtprodukts betreffe sowie nur eine absolute Ausnahmesituation, die Übertragung der Daten von einem alten auf ein neues Mobilgerät bei Wechsel des Mobilgeräts durch den Nutzer. Gleichzeitig würde ein Unterlassungsausspruch einen faktischen Vertriebsstopp der angegriffenen Ausführungsformen bedeuten.

84
bb) Die Klägerin unterstreicht, sie sei keine Patentverwerterin, sondern forschendes Unternehmen und Netzwerkausrüsterin, sowie als Markenlizenzgeberin auch indirekt am Smartphonemarkt beteiligt.

85
cc) Hiernach liegt keine Unverhältnismäßigkeit vor.

86
(1) Gemäß § 139 Abs. 1 S. 3 PatG ist der Unterlassungsanspruch ausgeschlossen, wenn die Inanspruchnahme aufgrund der besonderen Umstände des Einzelfalls und der Gebote von Treu und Glauben für den Verletzer oder Dritte zu einer unverhältnismäßigen, durch das Ausschließlichkeitsrecht nicht gerechtfertigten Härte führen würde.

87
Der Unverhältnismäßigkeitseinwand des § 139 Abs. 1 S. 3 PatG ist auf besondere Ausnahmefälle begrenzt. Dies trägt dem Umstand Rechnung, dass der Unterlassungsanspruch die logische Folge des Ausschließlichkeitsrechts ist. Mit der Erteilung des Patents entstehen an der patentierten Erfindung absolute Rechte, die neben ihrem Zuweisungsgehalt einen Ausschlussgehalt besitzen, so dass der Inhaber des Rechts grundsätzlich jedermann von der Nutzung der patentierten Lehre ausschließen kann. So erlauben sie insbesondere - im Rahmen der übrigen gesetzlichen, insbesondere der patent- und kartellrechtlichen Vorgaben - den Ausschluss Dritter von der Nutzung der patentierten Lehre. Um sein Ausschließlichkeitsrecht durchzusetzen, ist der Patentinhaber in aller Regel auf den Unterlassungsanspruch angewiesen.

88
Der Gesetzgeber hat in der Begründung des 2. PatModG klargestellt, dass eine Einschränkung des Unterlassungsanspruchs nur in besonderen Ausnahmefällen in Betracht kommt. Der Unterlassungsanspruch ist die regelmäßige Sanktion der Patentrechtsordnung bei einer Patentverletzung. Darlegungs- und beweisbelastet für eine Unverhältnismäßigkeit ist die Beklagtenseite. Eine Einschränkung des Unterlassungsanspruchs kommt nur in besonders gelagerten Ausnahmefällen in Betracht (BT-Drs. 19/25821, S. 53).

89
Wenn der Patentverletzer besondere Umstände darlegt, die im Einzelfall eine nicht gerechtfertigte Härte begründen können, kann es im Rahmen einer Gesamtwürdigung aller Umstände des Einzelfalls und bei einer sorgfältigen Abwägung aller Umstände unter Berücksichtigung des Gebotes von Treu und Glauben und der grundsätzlich vorrangigen Interessen des Verletzten an der Durchsetzung seines Unterlassungsanspruchs ausnahmsweise darauf ankommen, ob der Verletzte selbst Produkte oder Komponenten herstellt, die mit dem patentverletzenden Produkt in Wettbewerb stehen, oder ob primär eine Monetarisierung seiner Rechte das Ziel des Patentinhabers ist (BT-Drs. 19/25821, S. 53). Im Übrigen können wirtschaftliche Auswirkungen der Unterlassungsverfügung, die Komplexität von Produkten, subjektive Gesichtspunkte auf beiden Seiten und Drittinteressen zu berücksichtigen sein. So kann etwa zu Lasten des Verpflichteten eine fehlende Lizenzwilligkeit gesehen werden (BT-Drs. 19/25821, S. 54).

90
(2) Bei Anwendung dieser Maßstäbe greift der von der Beklagtenseite erhobene Einwand der Unverhältnismäßigkeit nicht durch. Unter Berücksichtigung aller Umstände des zwischen den Parteien geführten Rechtsstreits und ihrer maßgeblichen Interessen hat die Beklagtenseite eine Unverhältnismäßigkeit des Unterlassungsanspruchs nicht dargetan.

91
(a) Soweit die Beklagtenseite argumentiert, die Klägerin sei reine Patentverwerterin, kommt es hierauf für sich gesehen schon nicht an.

92

Denn nach der bisherigen Rechtslage (vgl. Werner, in: Busse/Keukenschrijver, PatG, 9. Aufl. 2020, § 139 Rn. 92 m.w.N.), der die Gesetzesbegründung zustimmt (s.o.), ist der Umstand allein, dass ein Patentverwerter einen Unterlassungsanspruch geltend macht, für sich gesehen nicht geeignet, diesen als unverhältnismäßig einzustufen. Unabhängig davon ist die Klägerin unstreitig mit eigenen Produkten am Netzwerkausrüstungs-Markt und als Markenlizenzgeberin indirekt auf dem Smartphone-Markt aktiv, wenngleich nicht im direkten Wettbewerb mit der Beklagtenseite im Bereich der Smartphones.

93
(b) Irrelevant ist auch, dass die Klägerin an dem Abschluss eines Lizenzvertrages interessiert ist. Zutreffend ist zwar, dass der Gesichtspunkt eines vorrangigen Interesses an der Monetarisierung von Patenten als ein Aspekt bei der Interessenabwägung zu berücksichtigen sein kann, wie oben dargetan. Dieser Aspekt steht im Zusammenhang mit der eigenen Marktteilnahme von Patentinhabern (oder deren Fehlen). … Sie ist auch nicht gehalten, bis zum Abschluss der Lizenzverhandlungen von der Einleitung eines Gerichtsverfahrens abzusehen, um dem Vorwurf einer Unverhältnismäßigkeit zu entgehen. Dann würde das Regel-Ausnahmeverhältnis, das § 139 Abs. 1 S. 3 PatG aufstellt, gerade in sein Gegenteil verkehrt, und das gesetzgeberische Ziel verkannt.

94
(c) Auch der Umstand, dass es sich bei den Verletzungsformen um komplexe Produkte handelt, führt hier im Einzelfall jedenfalls nicht zu einer Unverhältnismäßigkeit. Denn der Verletzer muss mögliche und zumutbare Vorkehrungen zur Vermeidung der Patentverletzung treffen und diese beachten sowie sich insbesondere so früh wie möglich um eine Lizenz bemühen (vgl. Werner, in: Busse/Keukenschrijver, a.a.O. § 139 Rn. 92 m.w.N.).

95
Die Unternehmensgruppe der Beklagtenseite hatte und hat, …, zum einen die Möglichkeit, ihr patentverletzendes Handeln durch Abschluss eines Lizenzvertrags zu legitimieren. Der von der Klägerin angebotene Lizenzvertrag erfasst …. Die Unternehmensgruppe der Beklagten hat dieses Angebot bislang nicht angenommen und damit mögliche sowie zumutbare Vorkehrungen zur Vermeidung der Patentverletzung nicht getroffen, insbesondere war sie - wie die Kammer in ihren Urteilen in den Verfahren 21 O 8879/21, 8890/21, 8891/21 und 11522/21 erkannt hat - nicht hinreichend lizenzwillig.

96
Zum anderen hat die Beklagte nicht zur Überzeugung der Kammer hinreichend dargetan, dass sie die Folgen des Unterlassungsanspruchs unzumutbar hart treffen würden. Dass die Klägerin ihre Patentrechte gegen einen lizenzunwilligen Patentverletzer durchsetzt und hierzu auf ein gerichtliches Verfahren angewiesen ist, ist dann bloß logische Folge. Dies begründet im Rahmen der gebotenen Gesamtbetrachtung dann aber keine Unverhältnismäßigkeit des Unterlassungsanspruchs.

97
(d) Auch die wirtschaftlichen Auswirkungen auf die Beklagtenseite führen nicht zu einem anderen Ergebnis. Die Beklagte nutzt das Klagepatent der Klägerin seit mehr als einem Jahr ohne Zahlung eines Entgelts und hat die Möglichkeit, einen Lizenzvertrag abzuschließen, der dem Unterlassungsanspruch entgegenstehen würde. Besondere Härten durch den Unterlassungsanspruch, die angesichts dieser Umstände zu einer Unverhältnismäßigkeit führen würden, hat die Beklagtenseite nicht dargelegt.

98
(e) Auch bei einer Gesamtschau der gegen die Verhältnismäßigkeit vorgebrachten Aspekte ergibt sich keine andere Wertung.

99
dd) Den Unterlassungsansprüchen steht daher die geltend gemachte Unverhältnismäßigkeit nicht entgegen. Ein angemessener Ausgleich in Geld nach § 139 Abs. 1 S. 4 PatG steht der Klägerin angesichts dessen nicht zu.

100
2. Der Anspruch auf Auskunft und Rechnungslegung folgt aus Art. 64 Abs. 1 EPÜ, § 140b Abs. 1, Abs. 3 PatG, §§ 242, 259 BGB.

101

a) Soweit die Beklagtenseite geltend macht, sie stellten die angegriffenen Smartphones nicht im Inland her, was für sich gesehen unstreitig ist, kann der Anspruch auf Auskunft und Rechnungslegung über die festgestellten Verletzungshandlungen hinausgehen, um die Klägerin in die Lage zu versetzen, Angaben der Beteiligten auch untereinander zu plausibilisieren. Sofern die Beklagten im Inland keine Verletzungsgegenstände hergestellt hat, kann sie dies mittels „Nullauskunft“ angeben.

102
b) Die Auskunftserteilung in elektronischer Form ist allgemein üblich, so dass sich der Auskunfts- und Rechnungslegungsanspruch hierauf erstreckt (dazu Zigann, in: Haedicke/Timmann, Handbuch des Patentrechts, 2. Aufl. 2020, § 15 Rn. 163).

103
3. Der Anspruch auf Rückruf und Vernichtung folgt aus Art. 64 Abs. 1 EPÜ, § 140b Abs. 1, Abs. 3 PatG. Der Anspruch auf Rückruf besteht auch gegen eine im Ausland ansässige Verpflichtete (BGH GRUR 2017, 785, 787, Rn. 33 - Abdichtsystem). Daher besteht der Anspruch auch hier gegen die Beklagtenseite. Ebenso besteht der Anspruch auf Vernichtung: Zwar liegt der Sitz der Beklagten im Ausland, sie liefert aber unstreitig Verletzungsgegenstände ins Inland und hat daher im Inland jedenfalls (mittelbaren) Besitz. Soweit die Beklagtenseite unterstreicht, eine Lieferung ins Inland bedeute keine Angaben zu Eigentums- und Besitzverhältnissen, hat sie eine reine Direktlieferung an Endkunden nicht dargetan. Wie eine Belieferung von Endkunden aber ohne ein zumindest bestehendes mittelbares Besitzverhältnis erfolgen soll, hat die Beklagtenseite nicht konkret dargetan.

104
Der Anspruch ist auch nicht unverhältnismäßig, § 140 a Abs. 4 PatG. Auch der Unverhältnismäßigkeitseinwand nach § 140 a Abs. 4 PatG ist auf enge Ausnahmen beschränkt (zum Vernichtungsanspruch siehe BeckOK PatR/Rinken PatG § 140 a Rn. 28, zum Rückrufanspruch BeckOK PatR/Rinken PatG § 140 a Rn. 46). Hier gilt das zum Unterlassungsanspruch Gesagte entsprechend.

105
4. Der Schadensersatzanspruch folgt aus Art. 64 Abs. 1 EPÜ, § 139 Abs. 2 PatG.

C.

106
Eine Aussetzung mit Blick auf die Nichtigkeitsklage vom 01.12.2021 (Anlage HL 1) nach § 148 ZPO ist nicht veranlasst.

107
I. Die Einleitung eines Einspruchsverfahrens oder die Erhebung einer Nichtigkeitsklage stellen als solches keinen Grund dar, das Verfahren auszusetzen. Anderenfalls würde man dem Angriff auf das Klagepatent eine den Patentschutz hemmende Wirkung beimessen, die ihm nach dem Gesetz gerade fremd ist (BGH GRUR 1987, 284 - Transportfahrzeug). Bei der gebotenen Interessenabwägung hat grundsätzlich das Interesse des Patentinhabers an der Durchsetzung des ihm erteilten Patents Vorrang (vgl. Cepl in: Cepl/Voß, Prozesskommentar zum Gewerblichen Rechtsschutz, 2. Aufl. 2018, § 148 ZPO Rn. 106 m.w.N.). Denn das Patent bietet nur eine beschränkte Schutzdauer. Für die Dauer der Aussetzung ist das Schutzrecht mit Blick auf den Unterlassungsantrag, der einen wesentlichen Teil des Schutzrechts darstellt, noch zusätzlich praktisch aufgehoben. Daher kommt eine Aussetzung grundsätzlich nur in Betracht, wenn die Vernichtung mit hoher Wahrscheinlichkeit zu erwarten ist (Cepl in: Cepl/Voß, a.a.O., § 148 ZPO Rn. 107 m.w.N.).

108
Beschränkt der Patentinhaber im Einspruchsverfahren sein Patent selbst oder verteidigt er es im Nichtigkeitsverfahren nur noch in beschränktem Umfang, und macht er diese eingeschränkten Anspruchsfassung im Verletzungsprozess geltend, so ist dies zwar zulässig (BGH GRUR 2003, 867 - Momentanpol I; GRUR 2010, 904 - Maschinensatz), kann aber dazu führen, dass eine Aussetzung als eher geboten erscheint (OLG München GRUR 1990, 352 - Regal-Ordnungssysteme).

109
Wird im Verletzungsverfahren nicht die erteilte Fassung eines Anspruchs geltend gemacht, sondern eine Kombination von Ansprüchen bzw. eine eingeschränkte Anspruchsfassung, ist mithin nur diese

ausschlaggebend für die Prüfung, ob eine Vernichtung wahrscheinlich ist (BGH GRUR 2010, 904 - Maschinensatz; OLG Düsseldorf GRUR-RR 2021, 69 - Decodieranordnung).

110
II. Nach diesen Maßstäben ist der Rechtsstreit nicht auszusetzen. Die von der Beklagten geltend gemachten Nichtigkeitsargumente greifen nicht durch.

111
1. Die Klägerin macht vorliegend nur noch eine weiter eingeschränkte Fassung der (bereits zuvor eingeschränkten) Ansprüche 10, 11 und 12 geltend, die entsprechend ihrem Hilfsantrag im Nichtigkeitsverfahren vom 02.09.2022 (Anlage K 26) jeweils um folgende Merkmale ergänzt sind:

„wherein the user data are user data from the another radio communication device (MS1) which are to be recovered on the radio communication device (MS2), and

wherein the user data comprise personal, private and highly sensitive data of the user of the radio communication device (MS2) such as saved messages, address book entries, calendar entries and credit card numbers."

112
2. Die Ergänzung der Ansprüche 10, 11 und 12 um die genannten Merkmale 3.3 und 3.4 stellt - entgegen der Ansicht der Beklagten - eine Beschränkung der Ansprüche dar.

113
Wie im Rahmen der Auslegung dargelegt (s.o.), geht der Begriff der Wiederherstellung der Benutzerdaten insoweit über deren bloße Übertragung von der anderen Funkkommunikationseinrichtung (MS1) auf die Funkkommunikationseinrichtung (MS2) hinaus, als die übertragenen Benutzerdaten auch verwendbar auf der Funkkommunikationseinrichtung (MS2) zur Verfügung stehen müssen. Hieraus folgt, dass die Ansprüche 10, 11 und 12 jedenfalls durch das Teilmerkmal, dass die Benutzerdaten „auf der Funkkommunikationseinrichtung (MS2) wiederhergestellt werden sollen", in Merkmal 3.3 einschränkt werden.

114
3. Die zusätzlichen Merkmale 3.3 und 3.4 sind - entgegen der Auffassung der Beklagten - auch hinreichend klar formuliert.

115
Die Beklagte hat diesbezüglich vorgebracht, der Begriff der „persönlichen, privaten und hochsensiblen" Daten in Merkmal 3.4 enthalte keine objektiv abgrenzbare Einschränkung, weshalb es dem Merkmal an Klarheit fehle.

116
Dieser Auffassung schließt sich die Kammer nicht an. Welche Benutzerdaten zu den persönlichen, privaten und hochsensiblen Daten i.S. von Merkmal 3.4 gehören, ist hinreichend klar bestimmbar sowohl aufgrund des allgemeinen Sprachgebrauchs dieser Adjektive als auch insbesondere aufgrund der beispielhaften Aufzählung derartiger Daten in Merkmal 3.4. Danach gehören hierzu (jedenfalls) „gespeicherte Nachrichten, Adressbucheinträge, Kalendereinträge und Kreditkartennummern", wodurch in [0002] und [0003] genannte Beispiele für persönliche, private und hochsensible Daten aufgegriffen werden. Eine objektive Auslegung des Begriffs der Begriff der „persönlichen, privaten und hochsensiblen" Daten ist daher unter Berücksichtigung dieser beispielhaft genannten Daten möglich. Dass - wie von der Beklagtenseite ebenfalls vorgetragen worden ist - eine beispielhafte Aufzählung in einem Anspruch für sich genommen keine einschränkende Wirkung entfalten kann, steht einer Berücksichtigung der Beispiele bei der Auslegung der Teilmerkmalen des Anspruchs, auf die sich die Beispiele beziehen, nicht entgegen.

117
4. Die Merkmale 3.3 und 3.4 sind auch ursprungsoffenbart.

118
Die Beklagte ist der Auffassung, die Anmeldeunterlagen offenbarten nicht, dass die zu entschlüsselnden Benutzerdaten solche sind, die auf der Funkkommunikationseinrichtung (MS2) wiederhergestellt werden sollen gemäß Merkmal 3.3 („user data (…) which are to be recovered on the radio communication device

(MS2)“, Hervorhebung hinzugefügt). Ursprungsoffenbart sei allenfalls das bloße Transferieren von Benutzerdaten von der anderen Funkkommunikationseinrichtung (MS1) auf die Funkkommunikationseinrichtung (MS2), aber jedenfalls nicht, was auf der Funkkommunikationseinrichtung (MS2) passiere. Die Beklagte verweist hierzu auf die Beschreibungsstellen [0003] und [0005], die jeweils - anders als Merkmal 3.3. - die Präposition „to“ und nicht „on“ verwendeten ([0003]: „In such a case user data is typically transferred or recovered from the damaged or failed device to the new device.“; [0005]: „Thus there is an obvious need for a more secure solution providing secure data transfer from a first radio communication device to a second radio communication device.“, Hervorhebungen jeweils hinzugefügt).

119
Dem ist nicht zuzustimmen. Wie im Rahmen der Auslegung dargelegt (s.o.), geht bereits aus der alternativen Nennung von Übertragung und Wiederherstellung in [0003] („transferred or recovered“, „data recovery or transfer“) hervor, dass es sich beim Wiederherstellen im Sinne des Klagepatents um etwas anderes als ein bloßes Übertragen handeln muss. Darüber hinaus offenbart die Erläuterung des Ausführungsbeispiels gemäß Figur 2 in [0031], dass die Wiederherstellung über das bloße Übertragen der Benutzerdaten hinausgeht, weil danach die Funkkommunikationseinrichtung (MS2) die „wiederherzustellenden Benutzerdaten“ empfängt („for receiving the user data to recovered“). Hierdurch wird verdeutlicht, dass der Wiederherstellungsvorgang in seiner Gesamtheit nicht mit dem Abschluss der Übertragung durch Empfang der Benutzerdaten bei der Funkkommunikationseinrichtung (MS2) endet, sondern zusätzlich jedenfalls einen nachgelagerten Aspekt der Wiederherstellung umfasst.

120
5. Der Gegenstand der Entgegenhaltung D1 (WO 01/41353 A2, Anlage MN 5 - D1) steht der Neuheit des Gegenstands der beschränkt geltend gemachten Ansprüche 10, 11 und 12 des Klagepatents nicht entgegen.

121
a) Die D1 offenbart ein Verfahren zum Versenden verschlüsselter Nachrichten von einem Sender an mehrere Empfänger über ein Kommunikationsnetz. Zur näheren Erläuterung der D1 verweist die Beklagte unter anderem auf die folgenden Figuren der D1:

122
b) Der Gegenstand der beschränkt geltend gemachten Ansprüche 10, 11 und 12 wird durch diese Entgegenhaltung nicht vorweggenommen. Es werden nicht sämtliche beanspruchte Merkmale gezeigt.

123
So offenbart die D1 jedenfalls nicht unmittelbar und eindeutig, dass die zu entschlüsselnden Benutzerdaten solche von der anderen Funkkommunikationseinrichtung (MS1) sind, die auf der Funkkommunikationseinrichtung (MS2) wiederhergestellt werden sollen (Merkmal 3.3). Wie dargelegt (s.o.), geht der Begriff der Wiederherstellung über das bloße Übertragen der Benutzerdaten von der anderen Funkkommunikationseinrichtung (MS1) auf die Funkkommunikationseinrichtung (MS2) hinaus und beinhaltet, dass die übertragenen Benutzerdaten auch verwendbar auf der Funkkommunikationseinrichtung (MS2) zur Verfügung stehen. Demgegenüber offenbart die D1 nur eine Lösung für das Versenden verschlüsselter Nachrichten und befasst sich nicht mit dem Aspekt, dass von der anderen Funkkommunikationseinrichtung (MS1) stammende Benutzerdaten, die - gegebenenfalls entsprechend fragmentiert - über die Transfereinrichtung (SERV) auf die Funkkommunikationseinrichtung (MS2) transferiert wurden, auf dieser verwendbar zu Verfügung stehen.

124
6. Schließlich übt die Kammer - unter Berücksichtigung aller konkreten Umstände des Einzelfalls und unter Einbeziehung des sämtlichen tatsächlichen und rechtlichen Vorbringens der Parteien - ihr Ermessen so aus, das Verfahren auch im Hinblick auf das übrige Vorbringen der Beklagtenseite, insbesondere gestützt auf die weiteren Entgegenhaltungen D2 (US 6,226,618 B1, Anlage MN 5 - D2) und D3 (Pawlan - Essentials of the

Java Programming Language, Anlage MN 5 - D3), nicht auszusetzen ist. Diese sind vom geltend gemachten Gegenstand des Klagepatents noch weiter entfernt als der Gegenstand der D1.

125
III. Da auch bei Zugrundelegung des eingangs erläuterten, abgesenkten Aussetzungsmaßstabs in Bezug auf eingeschränkte Patentansprüche eine Aussetzung nicht veranlasst ist, kommt es auf den Vortrag der Klägerseite im nicht nachgelassenen Schriftsatz vom 04.11.2022 zur Durchführung und zum Abschluss eines weiteren Beschränkungsverfahrens vor dem DPMA das Klagepatent betreffend nicht an. Eine Wiedereröffnung der mündlichen Verhandlung ist daher nicht veranlasst.

D.

126
I. Die Kostenentscheidung beruht auf §§ 91 Abs. 1, 100 Abs. 4 ZPO. Die mit der weiteren Beschränkung der Ansprüche einhergehende Teilklagerücknahme wirkt sich bei den Kosten des Verfahrens nicht aus, weil hiermit in Bezug auf die angegriffenen Ausführungsformen keine erhebliche Einschränkung verbunden ist (vgl. BGH GRUR 2012, 485, Rn. 19 - Rohrreinigungsdüse II).

127
II. Die Entscheidung über die vorläufige Vollstreckbarkeit beruht auf § 709 S. 1 und 2 ZPO. Die Festsetzung von Teilstreitwerten entspricht gängiger Übung der Verletzungskammern am Landgericht München I, wobei hinsichtlich Unterlassung, Rückruf und Vernichtung eine einheitliche Sicherheit zu bilden ist. Die Kammer schätzt die entsprechenden Teilstreitwerte dem klägerischen Interesse entsprechend wie im Tenor angegeben.

128
§ 712 ZPO ist nicht anzuwenden, weil die Beklagtenseite einen über die üblichen Nachteile einer Vollstreckung hinausgehenden, nicht zu ersetzenden Nachteil durch die Vollstreckung nicht dargetan hat.